REMARKS

This amendment is responsive to the above identified non-final Office Action. Claims 14 - 66 are now pending. Claims 14, 15 and 16 have been amended to more particularly point out subject matter which the Applicants regard as their invention. New claims 17 through 66 have been added. Support for the new claims 17 through 66 and for the amendments to claims 14 through 16 is found in the specification of the originally filed application. No new subject matter has been added.

Amendments to the Specification:

As mentioned above, the expression on page 12, lines 3-5, previously reciting,

"where

$$W_i = \prod_{j \neq 1} p_j ,"$$

has been amended to recite,
"where

$$w_i = \prod_{j \neq i} p_j"$$

The previous recitation of "j ≠1" is a typographical error. Support for the current recitation of "j ≠i" is provided on page 12, line 13 which provides the example for k=3 wherein "...$w_1 = p_2\, p_3$, $w_2 = p_1\, p_3$, and $w_3 = p_1 p_2$". It is noted in this example that each of the values w_i is determined by a product of values p_j where j ≠i.

As mentioned above, the expression on page 11, lines 3-6, previously stating,

"$Y_i = Y_{i-1} + [(M_i\text{-}Y_{i-1})\, (W_i^{-1} \bmod p_i) \bmod p_i] \cdot W_i \bmod n$

where
for i ≥ 2 and
$$M = Y_k, Y_1 = C_1, \text{ and } W_i = \prod_{j<i} p_j ."$$

has been amended to state,
"$Y_i \equiv Y_{i-1} + [(M_i\text{-}Y_{i-1})\, (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n$
where
for 2 ≤ i ≤ k, and
$$M = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j ."$$

Support for the amended expression "*2 ≤ i ≤ k*" is provided implicitly in the statement "$M=Y_k$", and in the fact the resulting message M is defined by Y_k, and because no value is

defined for $M=Y_{k+1}$, it is evident that $i \leq k$. Therefore, no new matter has been added by the amended expression "$2 \leq i \leq k$".

All of the other amendments to the specification provide corrections of obvious typographical errors and corrections to mathematical expressions in order to conform with more formal conventions for mathematical expressions that are well known to those skilled in the art.

Claims Rejections under 35 U.S.C. § 112

Claim 16 has been rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as their invention.

As a first basis for rejecting claim 16 under 35 U.S.C. § 112, the Examiner points out that claim 16 previously recited a term "$M_i/$" in an equation on line 23, the term "$M_i/$" being unknown to one of ordinary skill in the art. Applicants assert that recitation of the term "$M_i/$" was a typographical error. To correct this, claim 16 has been amended to replace the term "$M_i/$" with "M_i". Support for this amendment is found in the specification of the present application which correctly recites the equation on page 11, line 3.

As a second basis for rejecting claim 16 under 35 U.S.C. § 112, the Examiner asserts that the term "C_1" is left undefined and is unknown to one of ordinary skill in the art. In order to provide antecedent basis for the term "C_1", claim 16 has been amended to recite,

"…whereby

$$C_1 \equiv C \pmod{p_1},$$
$$C_2 \equiv C \pmod{p_2},$$
$$\vdots$$
$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$
$$d_2 \equiv d \pmod{(p_2 - 1)},$$
$$\vdots$$
$$d_k \equiv d \pmod{(p_k - 1)},$$

$$M_1{}' \equiv C_1{}^{d_1} \pmod{p_1},$$
$$M_2{}' \equiv C_2{}^{d_2} \pmod{p_2},$$
$$\vdots$$
$$M_k{}' \equiv C_k{}^{d_k} \pmod{p_k}"$$

-27-

Applicants point out that the term "C_1" is specifically defined in the specification (page 10, line 18, and page 10, line 21) of the present application which recites the simultaneous equations defining decryption sub-tasks for decrypting ciphertext C to obtain a message M, wherein the ciphertext has been encrypted using k=3 distinct primes p_1, p_2, and p_3 in accordance with one embodiment of the present invention.

Applicants thank the Examiner for the careful review of the claims. In view of the above described amendments and remarks, Applicants request that the rejection of amended claim 16 under 35 U.S.C. § 112 be withdrawn.

Claims 14 through 16 have been amended to more particularly point out subject matter which Applicants regard as their invention. Claim 15 has been amended to be an independent claim.

Non-Statutory Double Patenting Rejections:

Claims 14 through 16 have been rejected in the present Office Action under the judicially created doctrine of double patenting over claims 1 through 13 of U.S. Patent No. 5,848,159 (heretofore referred to as the issued patent). The Office Action asserts that claims 14 through 16, if allowed, would properly extend the "right to exclude" granted in the issued patent. This assertion is based specifically on an argument that claims 14 though 16 claims subject matter in common with claim 8 of the issued patent. Applicants respectfully disagree, and therefore traverse the non-statutory double patenting rejection.

Claim 8 of the issued patent refers to a "succession of invertible operations". The present Office Action asserts that these invertible operations refer to the same operations given by the equations recited in claims 14 through 16. To support this argument, the Office Action asserts that column 6, line 1 through column 7, line 33 of the specification of the present application, identifies the operations given by the equations recited in claims 14 through 16 as a succession of invertible operations. Applicants point out that there is no reference in this portion of the specification to a "succession of invertible operations".

Applicants assert that the "succession of invertible operations" recited in claim 8 of the issued patent is not equivalent to the equations recited in claims 14 through 16. There is no specific reference in column 6, line 1 through column 7, line 33 of the specification to the equations recited in claims 14 through 16 as a "succession of invertible operations".

106376.01   Atty Docket # 20206-25 (PT-TA 410 (Cont 1))

The "first ordered succession of invertible operations" recited in claim 8 of the issued patent actually refers to the equation recited in claim 7 from which claim 8 depends. Claim 7 recites in part "$C = a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$".

It is clear that the equation recited in claim 7 is different from the equations recited in claims 14 through 16 of the present application and the equations recited in column 6, line through column 7, line 33 of the specification. The "first ordered succession of invertible operations" recited in claim 7 provides for transforming C to M. The "second ordered succession of invertible operations" recited in claim 8 actually refers to invertible operations each of which is the inverse of corresponding ones of the first invertible operations recited in claim 7. The "second ordered succession of invertible operations" recited in claim 8 provides for transforming M to C. The equations recited in claims 14 through 16 of the present application provide a different method of transforming M to C and C to M. Therefore, neither of the first and second ordered succession of invertible operations as recited in claim 8 of the issued patent is equivalent to the equations recited in claims 14 through 16 of the present application.

For the reasons stated above, Applicants assert that claims 14 though 16 of the present application and the claims of the issued patent do not claim common subject matter. Therefore, Applicants request that the non-statutory double patenting rejection of claims 14-16 be withdrawn. Each of the new independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 recites substantially the same equations recited in claims 14-16. Therefore, Applicants further assert that each of the new independent claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 and the claims of the issued patent do not claim common subject matter.

Rejections Under 35 U.S.C. § 103(a):

Claims 14-16 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kawamura et al. (U.S. Patent No. 5,046,094) in view of Menezes et al. (pp. 89, 612, and 613 of the Handbook of Applied Cryptography).

Applicants understand the present Office Action to assert generally that the differences between the subject matter of claims 14-16 and the teachings of Kawamura et al. and Menezes et al. would have been obvious at the time the invention was made to a person having ordinary skill in the art of cryptography.

Each of the independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application recites a cryptographic scheme using a composite number n of the form

"... $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ where k is an integer greater than 2..." and where "... $p_1, p_2, ..., p_k$ are distinct prime numbers...." Therefore, each of the independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 recites a cryptographic scheme using a composite number having more than two primes (herein after referred to as a "multi-prime" cryptographic scheme).

The rejections of claims 14-16 under 35 U.S.C. § 103(a) are based on an argument presented by the Examiner which assumes: (1) that Menezes et al. teaches a multi-prime cryptographic scheme using a composite number n having more than two primes; and (2) that Kawamura et al. teaches an application of the Chinese Remainder Theorem to a conventional cryptographic scheme using two primes that is equivalent to the application of the Chinese Remainder Theorem to the "multi-prime" cryptographic scheme of the present invention. The Office Action states on page 6 that "[i]t would be obvious for one of ordinary skill in the art to modify the system of Kawamura et al. to have a modulus having the number of primes, 'k', being a number greater than two." Applicants disagree emphatically for the reasons discussed below.

I.   Neither Kawamura et al. nor Menezes et al., taken individually or collectively, teaches a "multi-prime" cryptographic scheme using a composite number n having more than two primes as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application.

The Office Action specifically states that "...Kawamura et al. lack a teaching that there can be more than two primes in the modulus...." Therefore, the rejections of claims 14-16 under 35 U.S.C. § 103(a) rely on an assumption that Menezes et al. teaches a cryptographic scheme using a composite number having more than two primes. However, the present Office Action does not actually state explicitly that that Menezes et al. teaches a cryptographic scheme using a composite number having more than two primes. The Office Action states on page 4 that "...[in] Menezes et al., there are *possibly* more than two prime numbers in the modulus n and they are called p_1, p_2, ..., p_n." Applicants point out that the modulus *n* is not a product of *n* primes, but is rather a product of *k* primes. It is not possible that the modulus n could be the product of n primes. The present Office Action further states on page 6 that "Menezes et al. teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to 3.2. Menezes et al. further teach that the integer factorization problem comes from factoring the product of multiple primes p-_1^e1 p-_2^e2 ... p-_k^ek, see

definition 3.3." While a reading of these statements seems to imply that <u>Menezes et al.</u> may possibly hint at a "multi-prime" cryptographic scheme using a composite number having more than two primes, it is evident that there is no affirmative statement in the Office action that <u>Menezes et al.</u> actually teaches or even suggests that such a scheme is possible.

Clearly <u>Menezes et al.</u> does not teach a "multi-prime" cryptographic scheme as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application. <u>Menezes et al.</u> is a well known textbook that describes conventional cryptography techniques and elementary number theory. The expression in <u>Menezes et al.</u> of the integer factorization problem (definition 3.3 recited on Page 89 of <u>Menezes et al.</u>) merely recites a fundamental theorem of arithmetic which states that: "$n = p_1^{e1} p_2^{e2} \ldots p_1^{ek}$ where the p_i are pairwise distinct primes and each $e_i > 1$" This fundamental theorem of arithmetic, which has been known for centuries, appears in every text book that addresses number theory. This theorem merely states that all numbers are either prime or composite, and that all composite numbers have a unique factorization as a product of powers of prime numbers meaning that a particular composite number cannot be formed as a product of a different set of primes. For the above explained reasons, Applicants assert that the expression "$n = p_1^{e1} p_2^{e2} \ldots p_1^{ek}$" does not even remotely suggest a solution to the problems associated with actually implementing a "multi-prime" cryptographic scheme using a composite number having more than two primes.

For the reasons stated above, Applicants assert that the Examiner has not cited any prior art reference suggesting the possibility of a multi-prime cryptographic scheme using a composite number having more than two primes. Even if there was an existing prior art reference suggesting a multi-prime cryptographic scheme using a composite number having more than two primes at the time that the invention was made, it would not have been obvious to arrive at a solution to the problems associated with implementing a multi-prime cryptography scheme based on a teaching of a conventional RSA-type cryptography scheme and the Chinese Remainder Theorem.

Neither <u>Kawamura et al.</u> nor <u>Menezes et al.</u>, taken individually or collectively, teaches a solution to the problems associated with implementing a multi-prime cryptography scheme. These problems include: (1) the necessity of developing and solving the k simultaneous equations, or sub-tasks, recited on page 10, lines 19-27 of the specification; and (2) the necessity of combining the results of the sub-tasks in an efficient manner. Furthermore, the Chinese

Remainder Theorem itself also does not imply any method or algorithm for solving these problems.

In accordance with the present invention, a solution to the problems associated with implementing a multi-prime cryptography scheme is provided by: defining k simultaneous equations, or sub-tasks (as expressed by the equations on page 10, lines 19-27 of the specification); solving the sub-tasks to provide results; and efficiently combining the results of these subtasks using either a recursive method (expressed by the equations on page 11, lines 3-6, of the specification), or a summation method (expressed by the equations on page 12, lines 3-5, of the specification). Each of the independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 recites these steps in a substantially similar form.

Neither <u>Kawamura et al.</u> and <u>Menezes et al.</u>, taken individually or collectively, teaches any solution to the problems associated with implementing a multi-prime cryptography scheme. Nor does the Chinese Remainder Theorem itself provide a solution to the problems associated with implementing a multi-prime cryptography scheme.

The Chinese Remainder Theorem is not actually a method or solution, nor does it imply any method or solution to any particular problem. The Chinese Remainder Theorem is simply a mathematical proof which proves the *existence* of a unique solution to specific types of problems. So, the Chinese Remainder Theorem in and of itself does not teach, hint, or suggest any solution to the problems associated with implementing a multi-prime cryptography scheme as taught by the present invention.

For the reasons stated above, Applicants assert that neither <u>Kawamura et al.</u> nor <u>Menezes et al.</u>, taken individually or collectively, teaches a "multi-prime" cryptographic scheme using a composite number of the form "... $p_1 \cdot p_2 \cdot ... \cdot p_k$ where k is an integer greater than 2...", as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application. Therefore, each of the independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 is patentable under 35 U.S.C. § 103(a) over <u>Kawamura et al.</u> in view of <u>Menezes et al.</u>

II. **It would not have been obvious at the time that the invention was made to combine a teaching of a "multi-prime" cryptographic scheme using a composite number having more than two primes (if one existed) with a teaching of an application of the Chinese Remainder Theorem to a conventional RSA-type cryptography scheme.**

Even if there was an existing prior art reference suggesting a multi-prime cryptographic scheme using a composite number having more than two primes at the time that the invention was made, it would not have been obvious to arrive at a solution to the problems associated with implementing a multi-prime cryptography scheme based on a teaching of a conventional RSA-type cryptography scheme and the Chinese Remainder Theorem.

Applicants point out that all RSA type cryptography schemes before that of the present invention used only two primes since their introduction which was at least as early as 1978. Various applications of the Chinese Remainder Theorem to conventional two prime RSA-type cryptography schemes have existed since at least as early as the publication in August of 1982 of the Quisquater reference which is cited but not relied upon in the present Office Action. From at least as early as 1978 until the time that the present invention was made in 1996, there was a need for an improved security and improved performance RSA-type cryptography scheme. Also, from at least as early as 1982 until the time that the present invention was made in late 1996, those of ordinary skill in the art of cryptography were very well acquainted with both two-prime RSA type cryptography schemes, and with applications of the Chinese Remainder Theorem to two-prime RSA-type cryptography schemes. However, there is absolutely is no evidence that a multi-prime cryptography scheme using a composite number having more than two primes was ever even contemplated prior to the time that the present invention was made in late 1996.

There was certainly a long felt but unsolved need for an RSA-type cryptography scheme providing improved security and improved performance. However, the Examiner has presented no references which even contemplate, much less actually implement, a multi-prime cryptography scheme as recited in independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application. Even if a multi-prime cryptography scheme had been contemplated prior to the time of the present invention, the problems associated with implementing such a scheme would have deterred practitioners from attempting to implement it. As mentioned above, these problems include: (1) the necessity of developing and solving the k simultaneous equations, or sub-tasks, recited on page 10, lines 19-27 of the specification; and (2) the necessity of combining the results of the sub-tasks in an efficient manner. As taught by the present application, the results of these subtasks may be efficiently combined using either the

recursive method (expressed by the equations on page 11, lines 3-6, of the specification) or the summation method (expressed by the equations on page 12, lines 3-5, of the specification).
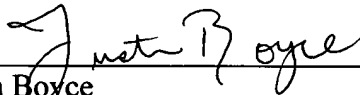
Advantages provided by the multi-prime cryptographic scheme of the present invention include enhanced cryptographic security and improved performance as explained in detail on pages 6 through 8 of the present application.

Accordingly, the teachings of <u>Kawamura et al.</u> and <u>Menezes et al.</u> are improperly combined, and even if properly combined, do not render obvious the claimed invention as recited in claims 14 through 66 of the present application.

For the reasons stated above, Applicants assert that independent claims 14, 15, 16, 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 of the present application are patentable under 35 U.S.C. § 103(a) over <u>Kawamura et al.</u> in view of <u>Menezes et al.</u> Claims 18-21, 23-26, 28-31, 33-36, 38-41, 43-46, 48-51, 53-56, 58-61, 63-66, 68-71, and 73-66 depend from patentable claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 respectively, and as such include all of the limitations of patentable claims 17, 22, 27, 32, 37, 42, 47, 52, 57, and 62 rendering them patentable also.

In view of the foregoing amendments and remarks, it is submitted that the application is now in condition for allowance and a notice of allowance of the pending claims 14 through 17 is respectfully requested. In the event that a telephone conference would expedite prosecution of the application, the Examiner is respectfully invited to contact the undersigned by telephone at the number set out below.

Respectfully submitted,
Dated: September 27, 2000
OPPENHEIMER WOLFF & DONNELLY LLP
3373 Hillview Avenue, Suite 200
Palo Alto, California 94304
Tel: (650) 320-4000
Fax: (650) 320-4100

Justin Boyce
Reg. No. 40,920

106376.01

SV: 106376 v04 09/27/2000
Atty Docket # 20206-25 (PT-TA 410 (Cont 1))